

## **REMARKS/ARGUMENTS**

The applicant acknowledges receipt, with thanks, the Office Action that was mailed on November 2, 2007. This amendment is responsive to the November 2, 2007, Office Action.

Presented herein are claim amendment and accompanying remarks. Claims 1 and 9 have been amended. The element that network access is denied until an actual authentication is performed using the provisioned security credential is not new matter as it is disclosed on page 11, lines 5-8 of the original specification. Claims 17-25 and 27 have been canceled without prejudice or disclaimer. Reconsideration of the application as amended is requested.

### **Claim Rejections – 35 U.S.C. § 101**

Claims 17-25 and 27 stand rejected for being directed to non-statutory subject matter, *to wit*: a computer program product and A computer usable medium. Withdrawal of this rejection is requested as these claims have been canceled without prejudice or disclaimer.

### **Claim Rejections – 35 U.S.C. § 102**

Claims 1-28 stand rejected as being anticipated by Funk (Paul Funk; Simon Blake-Wilson; “draft-ietf-pppext-eat-ttls-2.txt: EAP Tunneled TLS Authentication Protocol (EAP-TTLS)”); Internet-Draft PPPEXT Working Group (Nov. 2002). Withdrawal of this rejection is requested for reasons that will now be set forth.

The embodiments recited in independent claims 1 and 9 provide an in-band mechanism by which end-users can be provisioned with credentials without requiring any input beyond a username and password. First a tunnel is established between a client and a server. The tunnel may be established using Diffie-Hellman (DH) and be secured with a DH key agreement. As the tunnel may not achieve mutual authentication, an authentication, such as MSCHAPv2 is performed within the secure tunnel. If the authentication is successful, the client (peer) is provisioned with a unique credential. The only access allowed up until this point is between the client (peer) and server in order to enable the client to be provisioned with a secure credential.

Network access is denied until a successful authentication has been performed using the provisioned unique credential

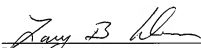
By contrast, Funk teaches using EAP-TTLS to gain access to the network. Once a successful authentication has occurred, keys are distributed and a session is initiated between the client and the network. Funk does not provision a secure credential and otherwise deny access to the network until a successful authentication is performed using the provisioned secure credential. Therefore, Funk does not teach or suggest each and every element of independent claims 1 and 9. Claims 2-8 and 28 directly depend from claim 1 and consequently contain each and every element of claim 1; therefore, claims 2-8 and 28 are not anticipated by Funk for the reasons already set forth for claim 1. Claims 9-16 are directly dependent from claim 8 and consequently contain each and every element of claim 8; therefore, claims 9-16 are not anticipated by Funk for the reasons already set forth for claim 8.

### **Conclusion**

Withdrawal of the rejections to this application as currently amended is requested for the reasons set forth above. If there are any fees necessitated by the foregoing communication, the Commissioner is hereby authorized to charge such fees to our Deposit Account No. 50-0902, referencing our Docket No. 72255/00006.

Respectfully submitted,

Date: 2-4-2008

  
Larry B. Donovan  
Registration No. 47,230  
TUCKER ELLIS & WEST LLP  
1150 Huntington Bldg.  
925 Euclid Ave.  
Cleveland, Ohio 44115-1414  
**Customer No.: 23380**  
Tel.: (216) 696-3864  
Fax: (216) 592-5009